



Protecting Content in the Digital Age

Balancing Creative Use with Creator Rights



Imagine the Ideal Digital Home

Buzz, the resident teenager, downloads songs from the Internet and plays them on his PC, his room stereo, or his portable player – a digitally emancipated man. His little sister has a multi-use copy of Disney's *El Dorado* on DVD that she can watch on the living room TV and digitally manipulate on the family PC. When mom runs, she takes a portable MP3 player loaded with her favorite songs. Dad unwinds on the deck with his laptop and a game, battling a friend across town.

Mom, dad, and the kids enjoy their music, movies, and games when, where, and how they want, while the companies that created the content are fully compensated for its use.

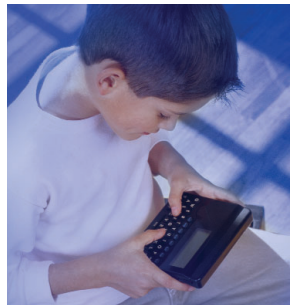
Multiple PCs, networked together and to the Internet, serve as digital hubs that channel content to numerous wireless appliances and devices – MP3 players, DVD players, laptop computers, PDAs, portable CD players and more. Content flows freely from one device to another, with no degradation of quality, no hassles and no copyright infringement.



The Digital Paradox

As with many technologies that preceded it, digital technology has been both a blessing and a curse to the content creation industries. Digital technologies enable movie studios to create animation, games, and special effects with incredible realism and impact. Digital reproduction allows studios to distribute their work with exceptional quality. And, digital music offers far greater clarity and purity than tape-based content. All these benefits translate into higher box-office and retail profits.

The downside of digital is consumers' ability to make near-perfect copies of music, videos, and games and distribute them en masse, without paying for them. Consumers don't want to be told how they can use their content or playback devices, nor do they want to bother with protection technology that forces them to comply with cumbersome procedures or prohibitions.



Intel is working to make digital content safe and flexible

Intel's Principles

As makers of the technology that powers the vast majority of PCs sitting at the center of digital content consumption, Intel has a strong interest in protecting both the rights of consumers and the property of studios. Our unabashed business interest is in selling Intel® Pentium® 4 processors, which are ideal “engines” for downloading MP3 files, editing digital video images, playing 3D digital games, and other types of digital content manipulation. However, we understand that our business model is dependent on a continuing stream of great digital content – games, music, and videos – that will compel consumers to buy these powerful PCs. Without adequate protection, content creators simply won't make great content available over digital networks.

Intel's business decisions are based around a core set of principles, which can be summarized as follows:

- **Intel respects intellectual property rights, and the rights of copyright holders.** Digital piracy threatens copyright industries, the emergence of exciting new digital markets, and, ultimately, consumer choice. We support the “balance” envisioned in the copyright law and the preservation of the public domain.
- **Intel is working to create a protected digital environment.** The fundamental elements of a protected environment are robust “protection at the source” encryption methods and establishment of a “protected digital domain” through link protection technologies. While content protection technology is a deterrent, it is not a perfect or complete solution to copyright infringement. Other key elements of a protected environment are consumer education, new business models, and the rule of law.
- **Content protection solutions should enable new flexible and portable media experiences that balance consumer expectations and right holder interests.** A protected digital environment ensures continued incentive for content providers and enables new consumer digital media experiences.

Content protection technologies should enable consumer choice, not dictate the availability of digital media experiences. Comprehensive disclosure (i.e., product labeling) is imperative to consumer choice and an effective digital marketplace.

- **Markets, not mandates, deliver consumer satisfaction.**

Legislative mandates stifle continued technological innovation, while effective markets yield compelling products, business models, and satisfied customers.

Doable but Difficult

Having said all this, the challenge of protecting digital content throughout its consumption cycle is far from trivial. Ensuring protection without compromising quality, ease of use, and performance is technically challenging and requires significant R&D investment. It also requires tremendous cooperation from information technology companies, consumer electronics companies, and content creators to balance the interests of consumers and studios, ensure interoperability, and deliver products that meet consumer demands for ease of use.

Much progress has been made, but much remains to be done. The market won't accept a single protection technology capable of safeguarding content throughout its entire distribution and usage lifecycle. Thus, the industry has created a suite of technologies that protect content as it travels over the Internet to a PC, from a PC to a TV, from one wireless device to another, from pre-recorded media to recordable media, and so forth. Technologies exist today for many of these phases of content consumption, but the industry continues to address unauthorized redistribution of content obtained from sources including the “analog hole” problem, terrestrial digital broadcasts, and unauthorized redistribution of content over peer-to-peer networks.

The Solution: Technology + Licensing

Effective content protection relies on both technological and legal mechanisms; technology cannot solve the problem on its own. Studios, consumers, and technology companies must come to an agreement about the rights of content owners and consumers – then, technology can enforce those rights.

Intel and other companies have been working collaboratively for several years to create a “chain” of protection for content as it is distributed to the consumer and flows from device to device within the consumer’s home. Each of the protection schemes includes both a technology element and a licensing element, with the licensing being critically important to the solution’s viability.

Content Protection Technologies

There are a number of technologies that content creators use to protect digital content “at the source” or point of origination:

- **The Content Scramble System (CSS)** protects video content distributed on DVD. CSS has been applied to nearly every DVD video disc released by the major Hollywood studios, making it the most widely used content protection technology for media.
- **Content Protection for Pre-recorded Media (CPPM)** (www.4Centity.com) is used to protect pre-recorded DVD audio content. Record labels encrypt content and license access keys to individual playback devices. CPPM provides a safe way for content creators to offer greater flexibility to consumers.
- Content delivered over cable and satellite is protected by **conditional access (CA)** technologies that encrypt content en route to the home. Although it is transmitted to the home across a generally unsecured transmission infrastructure, the content remains protected because it is encrypted. Devices such as a set-top box must be licensed to receive the key necessary to decrypt the content.
- Content delivered over the Internet is protected by a range of **digital rights management (DRM)** products made by companies such as Microsoft, Real Networks, IBM and others.

Protection within the home has been Intel’s principal area of focus, and we have participated in developing protection standards for both interconnects (networking) and physical media.

- **Digital Transmission Content Protection (DTCP)** (www.dtcp.com) provides protected transmission of audio/video content as it travels between digital devices over high-speed networks such as the IEEE 1394 standard. DTCP enables seamless content exchange between authenticated devices in the home through an encrypted exchange of content and copy control information (CCI).
- Intel also developed the **High-bandwidth Digital Content Protection (HDCP)** (www.digital-cp.com) specification to protect digital entertainment content across the DVI interface. It connects PCs and other devices to digital displays and contributes to safe, flexible, portable use of digital content.
- **Content Protection for Recordable Media (CPRM)** (www.4Centity.com), created by IBM, Intel, Matsushita and Toshiba, is a technology for protecting digital content on certain portable media formats such as recordable DVDs and SDCards.

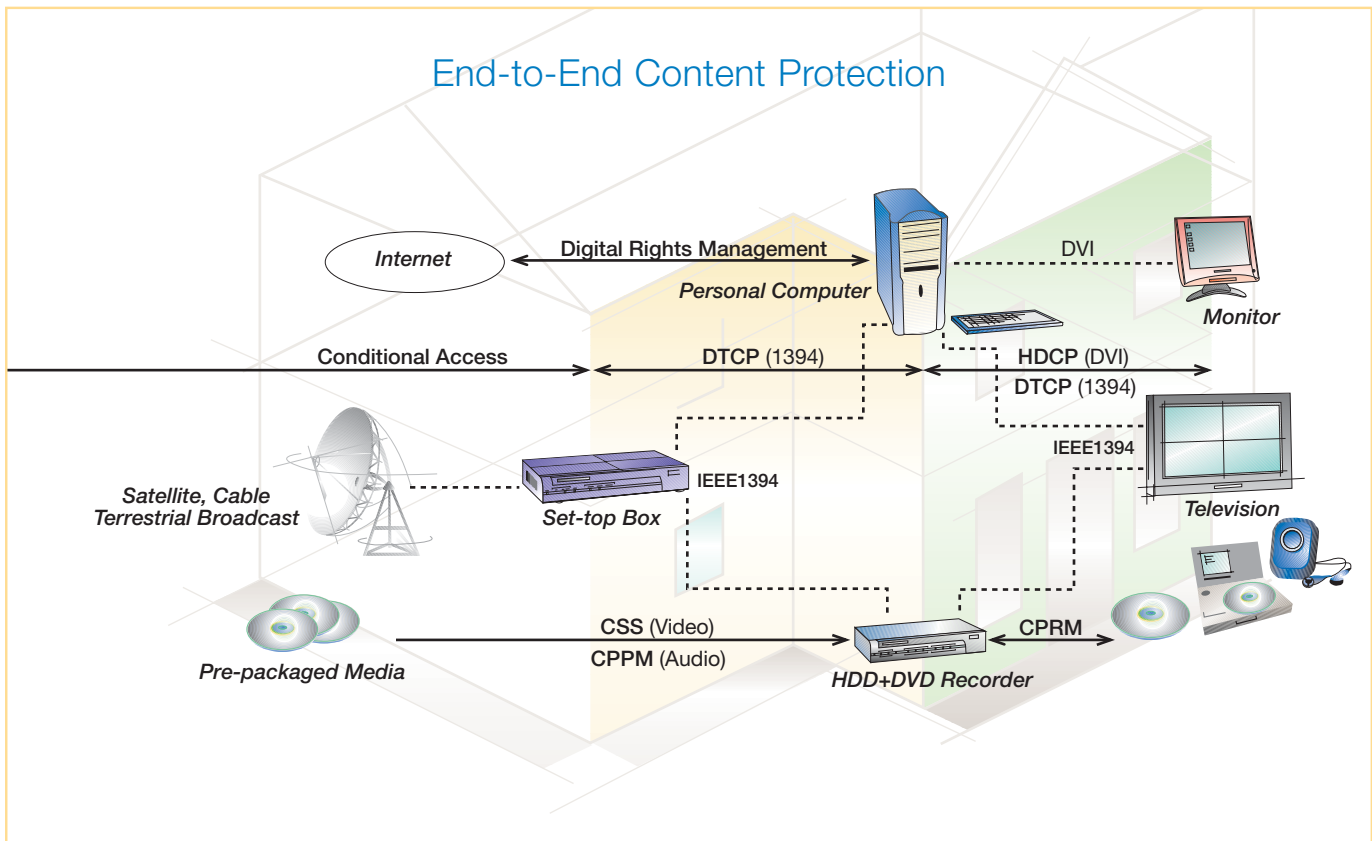
In addition to these individual technologies that protect content during specific phases of use, Intel and the 4C companies have drafted the Content Protection System Architecture (CPSA), which defines an overall framework for integrating many of these technologies as well as new technologies as they emerge.

Licensing Component

The licensing policy associated with each of these technologies is critical to their effectiveness. It is the legal mechanism that provides enforcement. All content protection specifications contain the following policy elements:

- **Compliance rules.** Compliance rules are technical documents embedded within the license that specify when and how subsequent protection technologies must be applied to content. Compliance rules can also include requirements such as encoding and carrying copy control information, response to watermarks, and limitations on the number or quality of permitted copies.





Technologies exist today to protect digital content as it enters the user's experience from the Internet, CD-ROMs, DVDs, satellite and cable, and moves from device to device.

- **Robustness rules.** Like compliance rules, robustness rules describe how devices must be designed and manufactured to make reverse engineering or modification difficult. Typically, separate rules apply to software and hardware implementation.
- **Renewability.** To maintain its effectiveness against inevitable attacks by hackers, a content protection technology must be renewable. Renewability is typically accomplished by updating the solution via downloadable software, using a removable hardware module such as a smartcard, or revoking devices that have been compromised.
- **Third-party enforcement.** The licenses provide the capability for content industry companies to seek an injunction or other damages against adopters who violate license provisions that directly relate to the technology's effectiveness.

Learn More

Protecting and extending the flexibility of digital content requires the cooperation of content creators, consumer electronics companies, PC manufacturers, and information technology companies. Everyone has a role to play in safeguarding content while it wends its way along the digital journey from source to consumption. No matter where your company touches this journey, get involved today, learning more and implementing your piece of the puzzle.

To learn more about:

DTCP, visit www.dtcp.com

HDCP, visit www.digital-cp.com

CPRM, CPPM and CPSA, visit www.4centity.com



Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Copyright © 2002, Intel Corporation. Intel, the Intel logo and Pentium 4 are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. *Other names and brands may be claimed as the property of others.